DESCRIPTION

Field of the Invention

This invention relates generally to purchasing systems via a public computer network system (Internet or World-Wide-Web). While the products sold on the Internet are often real and tangible, the market place exists in a virtual realm. To conduct the business of selling in the virtual realm of the Internet, a virtual transaction had to take place; or so it has been thought. This Invention utilizes non-virtual transactions that take place at a retail point of sale for a means of virtual merchandising.

Related Prior Art

Retail industries can exist anywhere. The historical version of retail was the actual retail point of sale. A retailer established a store where customers could visit, look at merchandise and make purchases. The customer had to visit the store in order to purchase the products. Other forms of retailing have existed like local street vendors, door-to-door salesmen, shop-by-telephone, mail order catalogs, infomercial shop-by-telephone, and most recently, the Internet.

To understand the difference between this invention and prior art, one must first be able to understand the differences between retail point of sale and other methods of sale. There is always a time variable involved with merchandising transactions, but one should not make the mistake of assuming that time is the essential element that distinguishes between direct purchases and those on account. The basic formula for establishing a credit account is where the purchase price (P) of a product can be paid at a later time (T), an interest rate (R) can be assessed, and the amount paid (A) = $P (I + R)^T$.

A person may gain extra time to pay for a purchase by using credit that one will extend to another that creates a credit account, but it is accomplished through an agreement between parties. Time has no meaning in the direct purchase formula (A) = P, For that matter, there is always some lag between the time payment is tendered and possession takes place even if for just split seconds. Sometimes a lag between payment and possession requires a voucher so that the purchaser has some proof that payment has been made. The voucher is usually just a simple sales receipt. Other times it can be a ticket such as for attending a theater or other engagement. The voucher used in RPOS does not represent an account or value of money. The voucher merely represents that the transaction has been completed and the merchandise, whether physical merchandise or simply entertainment, has been authorized.

Retail points of sale transactions involve at least one in-person contact with the buyer. On the Internet, it has always been assumed that this transaction must be conducted virtually on

James L. Dimon

the Internet; after all, the Internet is a virtual realm. With the huge rise in popularity the Internet, there are rising concerns from the public about who shall have rights to access certain Internet content such as but not limited to: materials with copyrights such as music, content that is adult in nature, or other restricted access material.

Regulatory authorities and web masters have made attempts to control access through the selling of access rights over the Internet itself. These services are often called subscription based I.D. or age verification services. User names and passwords or other means of secure access have been delivered to consumers after they entered credit card information. This has become an accepted means of control, particularly with Adult Verification systems.

Public Key infrastructure (PKI) is one method that has evolved into a secure and anonymous means of handling web transactions through the uses of encryption, trusted vendors, and trusted banking institutions. PKI methods of Web transactions involve digital signature and money transactions over the Internet. They require a customer, a bank, a merchant, a public archive such as an Internet web site, Certificate Authorization servers, and encryption and decryption of the data.

Most secure web transactions require cookies and Web delivered applets (such as JAVA, CGI, ASP) delivered to the user's computer via cookies. A cookie is information that a Web site puts on an end-users hard disk so that it can use the information at a later time.

In the past, there have been other Retail Point of Sale inventions that employ computer networks to deliver the authorization for the manufacture of media goods, but this RPOS system does not manufacture anything, it merely provides a prepaid entry ticket and tracing authority that gives the end user the permission to own the merchandise.

When the time comes time for the end-user to obtain the merchandise using the RPOS, each request for a Web product is already independent of all other requests. For this reason, the Web page server requires no additional input memory of the download transaction because all of that has taken place previously. The server does not need to know what pages it has sent to a user previously or anything about previous visits. No cookies are required to store its own information about a user on the user's own computer. For example, the Internet Explorer browser stores cookies in a Windows subdirectory. Netscape stores cookies as a single text file. RPOS does not require such a cookie system, but cookies may be used for other non-transactional features only if desired.

Retail Point of Sale Apparatus (RPOS) For Internet Merchandising is a return to the simplistic approach of pre-Internet ways of doing business, but it is not an obvious approach. As malicious attackers of Internet communications become more common, the Internet security

James L. Quinn

measures become increasingly sophisticated. The RPOS takes away some of the sophistication and uses much simpler yet effective technology in its place. The predefined transaction authorizes access to web content from a place off the web, originates at a real place of business, and is a concept that a trained Internet professional may not be able to grasp immediately; they have been conditioned towards more complicated means of accomplishing the tasks directly on the Internet.

RPOS would not negatively affect any electronic commerce as it currently operates. It would primarily be used in conjunction with current methods. A return to a retail establishment for conducting Web business may hold great promise for Internet security in the future. A search of past practices and inventions reveals a great deal of effort spent on avoiding over-the-counter transactions for Internet e-commerce rather than embracing it as does the RPOS technology.

Prior Art Differentiated

The field of Internet e-commerce has numerous existing patents. A complete search for prior history was not done prior to this filing but a few similar patents were found through a most basic search of the on-line patent databases. They are referred to below to help set the stage for one skilled in the art of Internet commerce to understand the differences between RPOS and previous methods.

This invention is not a Prepaid Internet Access Card, such as used to supply the purchaser of minutes on an Internet Service Providers (ISP) system, see US examples Patent Nos. 5,749,975; 5,987,612; 5,749,075, 5,987,430.

This invention is not merely a method for recording information on a card, computer disk, or other means of recording, see US example Patent No. 6,076,733. The method of recording might be bar code, magnetic tape, smart card, written inscription, or any means of recording information. This invention is not used to locate a specific URL, but is used to divine the predetermined transaction that provided access to a particular URL location.

This invention is not an organizational Internet access security system whereby business organizations control access to web content of their own employees or to others on a closed network or to generate personalized content pages for specific business purposes, see US Patent No. 6,076,166

This invention is not an Internet cash token system used as an anonymous means to get money to spend on the Internet. See US examples Patent Nos. 6,076,078; 6,072,870; 6,061,660; 6,042,149

This invention is not electronic-voucher system, which places a third party URL as the guarantor of funds. See US example 6,058,381.

James L. Duisen

This invention is not a mobile Internet media content delivery device in which the device itself carries the content. See US examples Patent Nos. 6,018,720.

This invention is not a means to preview merchandise and set up an account to purchase - as in US Patent No. 5,918,213, where the merchandise merely previewed at the point of sale, but then the transaction is conducted as an off the shelf purchase, through typical Internet methods, or phone-in-sale automated means. The retail point of sale apparatus for Internet Merchandising is a new means for conducting the actual transaction that could be added to such a system.

This invention is not a device for delivering media content through on-line programmable smart card authorization such as used in satellite television programming, or Web TV devices, where a home user of the system can call in on the telephone to order Pay-per-view programming. In these systems the smart card both receives and supplies data to the system over a private network. RPOS does not require programming after the initial over-the-counter transaction.

This invention is not a means to provide for manufacture of a material object at the location of purchase, see U.S. patent 4,528,643. The end-user (customer) has the choice of how to create the material object. RPOS merely provides the entry ticket for the customer to obtain the merchandise or media at their own leisure in the format of their choosing.

Although the user of the RPOS may be known, it can also be used completely anonymously. This invention is much like an event ticket to a movie theater or music concert except that the RPOS is specifically used for access (entrance) to Internet merchandising.

While RPOS can facilitate Secure Web Transactions, it is not a method of the transaction, merely a method of divining the existence of a predetermined web transaction. It does not require a trusted vendor, trusted bank, or buyer authentication. While RPOS may facilitate some of the same types of functions mentioned above if desired; it uses a completely new method.

This invention is essentially retail point of sale for the Internet. In order to best set the stage for a reader of this patent application to best understand the background of this invention and distinguish it from prior art, several descriptive names of the invention are listed below. This is not intended to be an exhaustive list but merely illustrates some of the ways such an invention can be used. After this list and for the remainder of this document, the Invention will be referred to as the RPOS. Although it involves a voucher system, the voucher need not remain in existence in all circumstances. RPOS can use a disk, paper ticket, memory stick, or any other means of supplying an access key and utility program.

Descriptive Names

James L. Quinn

1. Internet Content Voucher System
2. Cookie Free Cache Back System Card
3. Prepaid Card for Internet Content Media
4. Web Content Ticket
5. Over-the-counter Internet Sale
6. Simple Anonymity for Internet Content Delivery
7. Face-to-Face Verification System for Divining of Anticipated Internet Transaction
8. Non-Virtual Point of Sale for the Internet
9. Retail Point of Sale Card for Internet Content
10. Internet Authentication Card
11. Internet Adult Verification Card
12. Internet Allocation Card

The RPOS is an "actual point of sale" device for Internet content. Previous waves of invention attempting to satisfy the needs of secure web content on the Internet have delivered many "virtual point of sale" techniques and emphasis has been on the transaction itself and how to exchange money over the Internet.

When considering Prior art, the RPOS invention differs most noticeably from previous methods in the way it does not follow the trend to do everything on the Internet and uses "actual point of sale" as the place where a predefined Internet sales transaction takes place. The information provided by web delivered cookies or applets is not required by RPOS because the information is already included; it is hand delivered to the computer by the user.

Once media has been delivered and cataloged, further transfers may take place on the Internet using traditional Internet transactions, but the individual serialization of the RPOS transactions remains intact. The method of individual serialization is achieved through content-based identification and can be used for later RPOS transactions or any other subsequent Internet transaction.

Detailed Description

A security access key is provided in the form of a prepaid card sold as a retail item. The access key has a one time or multiple Internet session use as provided by the seller of the card. Through obtaining the CARD, the purchaser gains access to the website or specific web page(s) intended by the seller for either a defined duration of time or indefinite duration of time. Any time the end-user (customer) of the CARD is on the Internet, a very simple utility program may

James L. Dinan

be deployed to ensure that there are no changes to the cache content of the customer's computer and no cookies are accepted or transmitted during the delivery of the media content.

The utility of the invention is that it provides a method of controlling web access that requires at least one transaction be completed in person. No connection to a banking system for credit referencing is required, no vast system of computer networks is needed to verify anonymity and account status. The actual transaction takes place over-the-counter. The delivery takes place on a computer of the user's choice.

The CARD is a voucher system that is used only to authenticate that the user of the card is in fact the one in possession of it. The user of the CARD uses the CARD to access the content or merchandise from the computer of their choice. As the time required for the user holding the card to receive the desired content is decreased, the need for the CARD itself may become unnecessary for the acquisition of merchandise, but may be kept as proof of authorization.

The content itself may be recorded to disk compact disk, cassette, VHS tape, or other recording media of the user's choice. The media may be recorded at the point of sale location, but it is the choice of the user as to how the material object will be manifested.
The content that is recorded may be Internet content media or the content may be the purchase agreement for merchandise. When the content is a purchase agreement for merchandise, the payment can be made for the merchandise by the RPOS. The RPOS assumes responsibility for payment to the Internet vendor and the purchaser specifies the shipping address of such merchandise. The CARD in this situation may simply be a receipt of sale or other proof of payment.

Unlike any previous method of payment for Internet commerce in the past, there is no account, credit, or other means of electronic payment required for the buyer in the transaction. The proof is within the content itself because of the content based fingerprinting employed (see Content Fingerprint Cataloging below). The content becomes the verification of a sale.

Internet merchandisers such as but not limited to Amazon, Barnes and Nobel, Buy.com, Outpost, and others provide a verification page for each sale, which they intend to be printed by the user. These types of verification pages are excellent examples of specific URL information that can be determined ahead of time and sold whether it is for merchandise or content media.

When the purchase is for non-prepackaged merchandise such as content media, the media may be individually licensed with a unique serial number for protection against counterfeiting. Content fingerprinting is one of the methods used. Traditional digital signature may also be used, in situations where desired such as non media merchandise, but is not required or a part of the claims in this invention.

James L. Duane

Content Fingerprint Cataloging

Content fingerprint cataloging would be used for printing secure documents, discouraging unauthorized use, sending secret encoded messages, authentication of modification of documents, counterfeit detection, or other application requiring secure distribution of Internet materials. Content fingerprinting differs from digital signature or digital watermark in that the fingerprinting is not on the file itself but on the content of the file.

In the Industry of Internet publishing, one of the problems has been unauthorized copying, posting or otherwise revealing of sensitive materials for wide distribution. Millions of dollars in uncollected royalties are lost each year. Publishers have no way of detecting the responsible parties who willfully post the materials or otherwise "leak" the materials for wide distribution. The answer to the problem is a mechanism or way to "mark" individual copies of recorded material for licensing so the publishers can feel confident that appropriate royalties are being paid. The "mark" should be something not easily detected or removed.

Content fingerprinting techniques, historically, have most often been used in legal evidentiary scenarios. Most commonly, an media expert is called in as a witness to testify whether or not a particular sample of media is an original, a copy, or if it has some how been tampered with. For copyright infringement cases, particularly in black market (bootlegging) cases, the expert is usually not asked to testify about the media content, but more often testifies as to the packaging and whether or not the material object is indication of authorized or infringing copy. None of these methods is sufficient in today's scenarios where we must be able to determine who, how, and where, and when infringing copies came to be posted on media sharing websites.

The ability to recognize and catalog non conditioned audio tracks for fingerprinting is also not adequate for discriminating among huge lot sizes such as a platinum (million copy) selling album. Those differences that worked so well in legal evidentiary situations, telling one single media track from another, fall short in distinguishing one from a million virtually identical copies because the amount of data required in the database is simply overwhelming.

The RPOS database can consist of all the normally expected useful data fields for a cataloging system of authorized licensed users for a copyrighted work, e.g User Name, Last Known Address, Purchase Date, Audio Title purchased, etc. All of this information, and anything else that one could choose to contain within the database can all be indexed through a serial number. When watermarking is used in conjunction with fingerprinting, there is no need to store in the database a copy of the media track, information about the media track fingerprint,

James L. Duncan

or include an indexing system capable of finding all of those properties. All that is needed is the serial number because that particular information is always piggybacked right along with the possibly infringing media itself.

This document suggests just some basic methods of fingerprinting Internet content: Font Fingerprinting, hidden pixelization, concealed ASCII, and non-visible/inaudible codification. While these methods of preconditioned fingerprinting are provided as a basis for explaining the best use of the RPOS, the actual preconditioning (watermarking) techniques are not part of the claimed invention, merely a necessary step in developing the content based identification catalog system. The catalog system, on the other hand, is an essential part of the claimed invention.

Font Fingerprinting

Bar codes are typically comprised of black and white stripes, yet all that a bar code really represents is a binary code. For Font Fingerprinting of Internet content, hidden binary codes are placed into documents so that a specific record of the content travels with the document. It is much different from digital signature, for example, where the file itself is tagged and encrypted and can't be read unless the proper keys are used to decrypt the message. For fingerprint marking of the document, the mark stays with the document even after it is properly received and possibly changed.

A base font is modified only slightly so as to not be immediately noticeable to the human eye, yet enough for machine recognition. The base font becomes the "0" of the binary and the modified font is the "1". Any text string can be modified to imprint a binary coded binary (BCB). The decoding is later accomplished using a scanner with a character recognition system capable of distinguishing the font differences.

Font fingerprinting is particularly designed to be most readily used for printed media, but the fingerprinting could also follow a soft copied document provided the file format remains Rich Text Format (.RTF) or better, giving access to the font aberrations. The font set used for printing the "fingerprinted" document must also be available to the computer that receives the document. Future developments could include a highly compressed file format capable of self-decompression that would mask the fact that the distributed font set is traveling with the document.

Another method of sending a font generated BCB with a softcopy document, not requiring a font subset file, mixes two available fonts that are a close match such as Courier New with 11 point font and Courier 10 BT with a 10 point font.

Courier New: abcdefghijklmnopqrstuvwxyz

Courier 10 BT: abcdefghijklmnopqrsruwxyz

James L. Dimon

Mixed: abcdefghijklmnopqrstuvwxyz

(this barcode reads 10101010101010101010101110 because the a,c,e,g,i,k,m,o,q,s,u,w,x, and y are printed in courier 10 BT, and the remaining letters are printed in Courier new.

While this combination is visible to the naked eye through close examination, the text is not noticeably different unless you know what you're looking for. It was just an attempt at finding a good match, but there may be other good system fonts that are a close enough match and are truly invisible to the naked eye.

Hidden Pixelization

The format of choice for delivery of images over the Internet has been the jpeg, formally the ISO standard 10918, which keeps the file size for delivery fairly small. All digital images currently used on the Internet are made up of tiny pixels. For hidden pixelization, a digital image is converted to a similar image of a higher resolution (more pixels). In other words any single pixel in the original image is recreated as multiple pixels all of the same color. For example a 320 x 240 = 76, 800-pixel image becomes a 640 x 480 = 307,200 pixel image, or roughly four pixels per one pixel of the original image.

Several of the pixels from these new higher resolution images can then be encoded with a BCB by varying the shades within the 4 pixels only slightly - leaving the neutral color of the original larger pixel essentially unchanged to the human eye. Any documents delivered over the Internet that contain these images are thereby permanently marked.

This re-pixelization creates four available binary codes in the original pixel. The original color is the "0" code and the slightly changed shade is the "1" of the binary. One of the keys to making this system less detectable is to disguise the encoding by causing the encoded digital file to still report to the user that it is still a 320 x 240 image when in fact it has been changed to a 640 x 480 image and then report back to the viewing system the proper resolution. If the user resaves the image into a different format such as GIF, the code may or may not be transferred, but as long as images in documents are untouched, the document remains fingerprinted.

Concealed ASCII

ASCII stands for American Standard Code for Information Interchange. ASCII was developed a long time ago and the characters are not always used in the same way on different computer systems. ASCII was originally designed for teletypes and the first 31 characters in today's applications are no longer used as originally intended. Concealed ASCII finger printing

James L. Davison

takes advantage of the fact that several of them act the same as the ASCII character "032" in many applications. ASCII 32 is the code for a blank space.

ASCII characters 0, 10, and 13 do not display anything on most Windows applications. Character 9 will move to a tab, making a long blank space. 16-25 and 27-31 produce a black area on the screen in some applications and a blank area in others. So do 1-9, 11, 12, 14, and 15 on some Windows applications-, however, they often cause error messages in the compiler for many applications. Concealed ASCII can create a BCB by using the standard ASCII 32 in spaces as the "0" character of the binary and an alternate ASCII 0, 10, or 13 with ASCII 32 as the "1" character of the binary.

Example: The quick gray fox jumps over the lazy brown rabbit.
There are nine spaces to use for the BCB in the preceding phrase. The code in the example above reads 010000111. The code for the 2^{nd}, 7^{th}, 8^{th}, and 9^{th} spaces in the phrase is ASCII 10 followed by ASCII 32. The remaining spaces simply use ASCII 32. While the concealed ASCII fingerprinting is not printable, it can be used to travel with text of a printable document

Concealed ASCII can easily be lost when transmitted as plain text over the Internet and other systems, but many documents are transmitted over the Internet in specific file formats that would maintain specific ASCII sequences not visible to the reader without looking to the particular codes that generated the text.

While concealed ASCII is not truly content based, (it is on file not the content), it approaches content based because it is not merely concealed in the file header, but is spread throughout the document.

Non-visible or Inaudible Codification

Analog (content based) signals of non-discernable frequencies for human ears or eyes are individually dubbed into media recordings, which can later identify the origin of the recording. The sights or sounds are created using a frequency, signal generator, or other means of creating analog signals. The analog signals which cannot be heard or seen by humans, can be used for distribution of copyright materials such as mp3 music or dubbed into the soundtrack of a video that is distributed on the World-Wide-Web (Internet).

Identical songs or videos by the same artist can become individual versions that are licensed to individuals. Using sensitive digital software and computer sound editing tools available from a number of manufacturers the sights and sounds outside the range of human discernment can later be detected to verify if the recording is in fact licensed and who is the

James L. Quinn

owner of the license. The signals essentially encode any individual identification to a song, video, or other media that contains audio or video tracks.

The human sound range is between 20 and 20,000 hertz for a young person and much less for an old person. The human visual range for light lies within a range around 109 MHz. Visual analog signals can also be dubbed into digital video recordings. The key to non-visible or Inaudible Codification is merely that that signals are dubbed into the content and not just on the file itself

Content Fingerprint Cataloging Usefulness

Preconditioned Fingerprint Cataloging of documents is a useful and new idea. The usefulness of the specific methods for marking as shown above is greatly diminished when patented and disclosed to the public. The actual methods of fingerprinting (watermarking) really should be kept as "Trade Secrets". The above methods are not fool proof or even sophisticated enough to hold up against even the least sophisticated of hackers. They are merely offered here as examples of how a fingerprint catalog can best be used to individually license Internet materials. As industry looks to the Internet for delivery of every kind of copyrighted material, there will be other specific methods of fingerprinting. Since, nobody is working on this type of copyright protection; the concept itself might be of strategic advantage because Fingerprinting Internet delivered media may involve documents, images, videos, sound tracks, or any other type of media that can be produced for the Internet.

Description of Drawings

The following drawings provide examples of different applications and construct specifications for the RPOS technology. They are not meant to be inclusive of all uses, they are merely examples. They are given as flow charts and schematics which are not specific mechanical drawings; thus the parts of the drawings are not individually numbered and are provided merely to help in understanding of the invention to one reasonably skilled in the art.

Figure #1 uses a flow chart to illustrate a use of the RPOS. The process begins with web content dealers who have content posted to a public computer network (Internet) and have chosen to use RPOS for distribution. The web content dealers may manufacture the card themselves or use a third party. The type of security system used for placing the access key on the card is only important as to the particular level of security that is desired. The web content dealer then distributes the CARD, directly or through distribution channels, to a retail establishment. The retail establishment sells the CARD over the counter to the customer. The

James L. Duncan

dealer, distributor, and retail establishment may use whatever profit margins or price mark-ups as they choose or is agreed upon. The CARD is delivered to the customer like any other retail product. Continuing along the flow chart in Figure #1 to the customer, the CARD is used to access only the web content that is predefined by the CARD. The purpose of the CARD in this transaction is only to ensure that the user is in possession of it. The transaction takes place through an over-the counter sale.

Figure #2 uses a flow chart to illustrate an alternate use of the RPOS which is the construct specification for claim 3 in this application. The process again begins with Web Content Dealers. In this application the Web Content Dealers may or may not subscribe to the RPOS system (i.e. make their own CARDs). To facilitate the creation of a CARD for the Content Dealers, a retail establishment supplies a computer or terminal as a customer access point, which provides Internet access, and issues a CARD to a customer upon entering the retail establishment. The customer browses the web and looks for content to purchase. Whenever a Web Content Dealer requires some sort of payment and the customer agrees, the customer authorizes payment from the retail establishment and by default the retail establishment agrees to the purchase. The customer is not required to enter his or her own name, credit card payment information, address, or any other information that they do not choose. Upon leaving the establishment, the customer pays the retail establishment the amount required for content received or to be received. The purpose of the CARD in this transaction is only to ensure that the user is in possession of it. The actual transaction takes place through an over-the-counter sale.

The processes described in figure #2 illustrates a subtle yet important difference from prior art used in Internet commerce, in that Internet access is only desired when the customer is attempting to choose which media content to purchase. The customer can later retrieve the media on whatever computer or network port the customer chooses. Internet access is not required during the recording of specific media content locations (URLs); they can be simply written down, picked out from a written menu after having seen the web dealers preview pages, or retrieved as a menu item from the local computer at the check out. Internet access is also not required during the recording of the specific access information, or during the retail transaction. While Internet Access during these processes may be used to facilitate the RPOS processes, it is not required. While the CARD holds some intrinsic value it does not hold any dollar amount information, account information, or other means of payment; the transaction is completed in person at the checkout.

Figure #3 uses a flow chart to illustrate an alternate use of the RPOS. The process again begins with Web Content Dealers. A Vending Machine Dealer purchases CARDs through

James L. Dickson

normal product distribution channels. Customer purchases the CARD from the vending machine acquiring the ability to access the desired web content. This type of system is not capable of age verification as with over-the-counter sales. Again, the purpose of the CARD in this transaction is only to ensure that the user is in possession of it. The actual transaction takes place through a vending machine.

Figure #4 illustrates how the CARD is used as an age verification system (Adult Check). The process begins with dealers of adult materials on the Internet. A retail establishment (such as video rental store, convenience store, bookstore, adult merchandiser, or other type of store) obtains CARDs through typical distribution channels. Customers purchase the CARD over the counter provided they can prove they are of legal age to do so. Customer physically transports the CARD to a location where customer has access to a computer that is capable of receiving Web content. The customer uses the CARD to obtain access to those specific materials the seller of the CARD intended.

Figure #5 is a flow chart for programming the small security application (cache back/cookie free) that helps control security and anonymity.

Figure #6 shows some examples of recording devices that are used or could be modified for use as the media delivery method, access CARD, or to deliver the small cookie-free-cache-back application.

Figure #7 is an example of Font Fingerprinting where a font subset file must be delivered to the user.

Figure #8 shows a schematic of how pixels are laid out in a typical bitmapped or other digitally formatted image as an example of Hidden Pixelization for Content Fingerprinting.

Figure # 9 illustrates the similarities between the New Courier font and the Courier 10 BT font.

James L. Quinn

CLAIMS

1. A purchasing system for Internet merchandise or media, comprising:
customer access point at a retail point of sale establishment;
said establishment acts as seller through an in-person transaction with said customer;
means for customer, seller, said establishment, or any other party to provide the specific URL information that is the location of Internet merchandise or content desired by the customer;
means for predetermining such URL that consists of a predetermined Internet Transaction;
means of accepting payment whether it be cash or credit;
means of conducting purchase of Internet merchandise on behalf of said customer including entering payment from said establishment as an intermediate purchaser or other means of distribution to said establishment,
means of storing, retrieving, or shipping of said Internet merchandise;
means of transfer of ownership of said Internet merchandise by access privileges given to said customer.

2. Method of claim 1 for providing a level of security in predetermining an Internet Transaction and access privileges for prepaid media content over a public computer network (Internet) using a computer, comprising;
media Content on a public computer network (Internet),
creating or procuring a card, computer diskette, or other means of record;
writing, inscribing, programming, or otherwise placing access information on the card, computer diskette, or other means of record without requiring access to a public computer network (Internet) during the recording process whether or not access is actually made;
using said card, computer diskette, or other means of record as a location for stored information, purchasing or other transfer of ownership of said card, diskette, or other means of record through a retail transaction (non-virtual point of sale) without requiring access to a public computer network (Internet) during said transfer whether or not access is actually made;
said retail transaction whether or not payment consideration is exchanged, i.e. said transaction that may include free samples;
physically transporting said card, diskette, or other means of record to a computer or other receiving device for a public computer network (Internet);
using the card, diskette, or other means of record to retrieve said stored information;
using said stored access information for obtaining media content from a public computer network (Internet).

James L. Quinton

3. Method of providing a level of security in claim 1 means of transfer of ownership for prepaid media content over a public computer network (Internet) using a computer which individually encodes license, serial number, or other identifying mark through content fingerprinting, comprising:

first a visible, audible, or otherwise humanly detectable label version of serial number, coded license number, or other identifying mark;

a second label that is only machine visible, audible, or otherwise detectable version of serial number, coded license number, or other identifying mark;

said machine only visible, audible or otherwise noticeable label consists of a coded message capable of singularly distinguishing the content from other content of the same or similar type;

means of recording, writing, or otherwise distinguishing said machine visible or audible code on said Internet media content for content fingerprinting purposes.

4. Method of providing a level of security in claim 1 means of transfer of ownership for prepaid media content over a public computer network (Internet) using a computer, comprising;

individually coded license, serial number, or other identifying mark through content fingerprinting that uses a code visible or audible otherwise noticeable only by a machine on the said first mark that is a first private key of a first public/private key pair to indicate that said merchandise is authentic and said second label is a second private key of a second private/public key pair used to authenticate the delivery of said merchandise.

5. A method transfer of ownership of Internet media of claim 1 by anonymous download (retrieval) of media content over a public network (Internet), comprising;

placing a small amount of programming code (application) on a card, computer diskette, or other means of record;

writing said small amount of programming code (application) to perform the function of adjusting the security settings of a computer or other receiving device for a public computer network (Internet) including, capturing current Web browsing cache content status (temporary storage capability including memory and disk cache),

capturing a computer's current operating system recent document content status,

temporarily turning off cache capability for web browsers,

temporarily turning off cookies (ability for remote computers to store information),

temporarily turning off web delivered applet capabilities (e.g. JAVA, CGI, ASP),

returning cache content status, operating system recent document status, cache capability settings, cookie enabling settings, or other settings changed by application to original state before application was run on said computer;

James L. Davison

retrieving preconditioned content identifiable media over a public computer network (Internet) during such instance that said application (above) has adjusted the said security settings of said computer.

6. Apparatus of Claim 1 for customer access point comprising a store, kiosk, or other customer access point with a computer with or without Internet access that includes a digital storage device such as hard drive, music or other media content in digital form on said hard drive, a recording device such as but not limited to CD Bumer, DVD Bumer, VHS TAPE Recorder, Cassette tape recorder.

7. Apparatus of Claim 1 for customer access point comprising; a store, kiosk, or other customer access point with a computer with or without Internet access that includes a printer to provide means for transfer of ownership of claim 1 of said Internet content by providing said access information of claim 1 by means of a ticket, card, paper, or other recorded media of said access information.

8. Means of claim 1 for said establishment to store, ship, or retrieve said Internet media might be performed by said customer, said establishment, original seller of the merchandise, or other potential party not mentioned.

9. A method transfer of ownership of Internet media of claim 1 by recording such media on a recording device such as but not limited to a CD burner, DVD burner, VHS TAPE recorder, or cassette tape recorder by said customer at the location of said retail establishment, or other location of choice.

10. A method transfer of ownership of Internet media of claim 1 by recording the URL information and a specific access code to the URL onto portable device capable of storing said information.

11. Means for audio, video, text or other content media recording that includes the ability to dub, loop, mix, otherwise detect or add signals existing in content to individually identify and catalog a recording which:

said signals are outside of the frequency range for human discernment,

said signals are for the purpose individually identifying the origin of the recording,

said signals are a code such as binary, morse, or other signal device,

said signals are looped, dubbed, mixed, digitally added or otherwise detected or added to the sound or video stream,

said signals are individualized when added to multiple recordings of content that create technically different recordings which are essentially identical to the human perception.

James L. Quinn

12. Product of audio and/or video recording of claim 11 which is used to catalog, determine licensing, or serial number identification of materials communicated over a public computer network (Internet).

13. Means for providing a user identifier to identify one or more recipients of Internet media content (content fingerprinting) comprising the steps of:

creating or detecting a label, version number, serial number, coded license number, or other identifying mark;

converting the label, version number, serial number, coded license number, or other identifying mark to machine only visible/audible detectable version of serial number, coded license number, or other identifying mark;

dubbing, looping, writing, programming, placing or otherwise detecting said machine only visible/audible code on previously existing media content;

cataloging, indexing, databasing, or other means of creating a sequential record of said label;

said machine visible label consists of a coded message capable of singularly distinguishing the content from other content of the same or similar type;

said machine visible coded message is binary, Morse, or other discernable code form;

means of recording, writing, or otherwise placing said machine only visible/audible code on said Internet media content;

means of reading said machine only visible/audible code on said Internet media content to divine its serial number or other identifying information.

James L. Davison